DPI Application Security Manager (ASM)

A User Guide for District Security Administrators and
Application Administrators

TABLE OF CONTENTS

This user guide will not be helpful for you unless **(1)** you have a WAMS ID and **(2)** you have been given access to Secure Home as a District Security Administrator or Application Administrator.

- If you need a WAMS ID visit: https://on.wisconsin.gov/WAMS/home.
- If you think you already have access as a District Security Administrator but are unsure, go here: https://apps2.dpi.wi.gov/ldsutil/admin/.
- If you are a principal, teacher, CESA administrator or other user and already have a WAMS ID, contact the appropriate district Application Administrator for access: https://apps2.dpi.wi.gov/ldsutil/admin/.
- If your district does not have a District Security Administrator, have your District Administrator submit a District Administrator Authorization Form and indicate the District Security Administrator(s) for your district here: https://helpdesk.dpi.wi.gov/DistrictAccess.html.

1. APPLICATIONS AVAILABLE WHEN LOGGING IN TO SECURE HOME

DPI Application Security Manager (ASM)

This tool allows District Security Administrators and Application Administrators to securely assign or revoke user access to data reporting tools and reports stored in Secure Home.

Multi-Dimensional Analytic Tool (MDAT)

This application allows authorized users to create reports comparing student achievement over time utilizing WKCE and other data sources. MDAT provides authorized users the capability to analyze student-level information as well as to compare to district and state averages.

Multi-Dimensional Analytic Tool (MDAT) Training Version

The MDAT Training version contains fictitious data and should be used for presentations and training purposes. The goal of this version of the tool is to enable hands-on training sessions to be held for a variety of users at one time while ensuring student data remains confidential.

IEP: Postsecondary Transition Plan (PTP)

An application that guides authorized IEP team members through the postsecondary transition requirements (form I-8) by responding to a series of inquiries and questions.

School Directory

This application allows users to view and update the district and school universe which all major DPI applications use. The data appears in DPI's school directories.
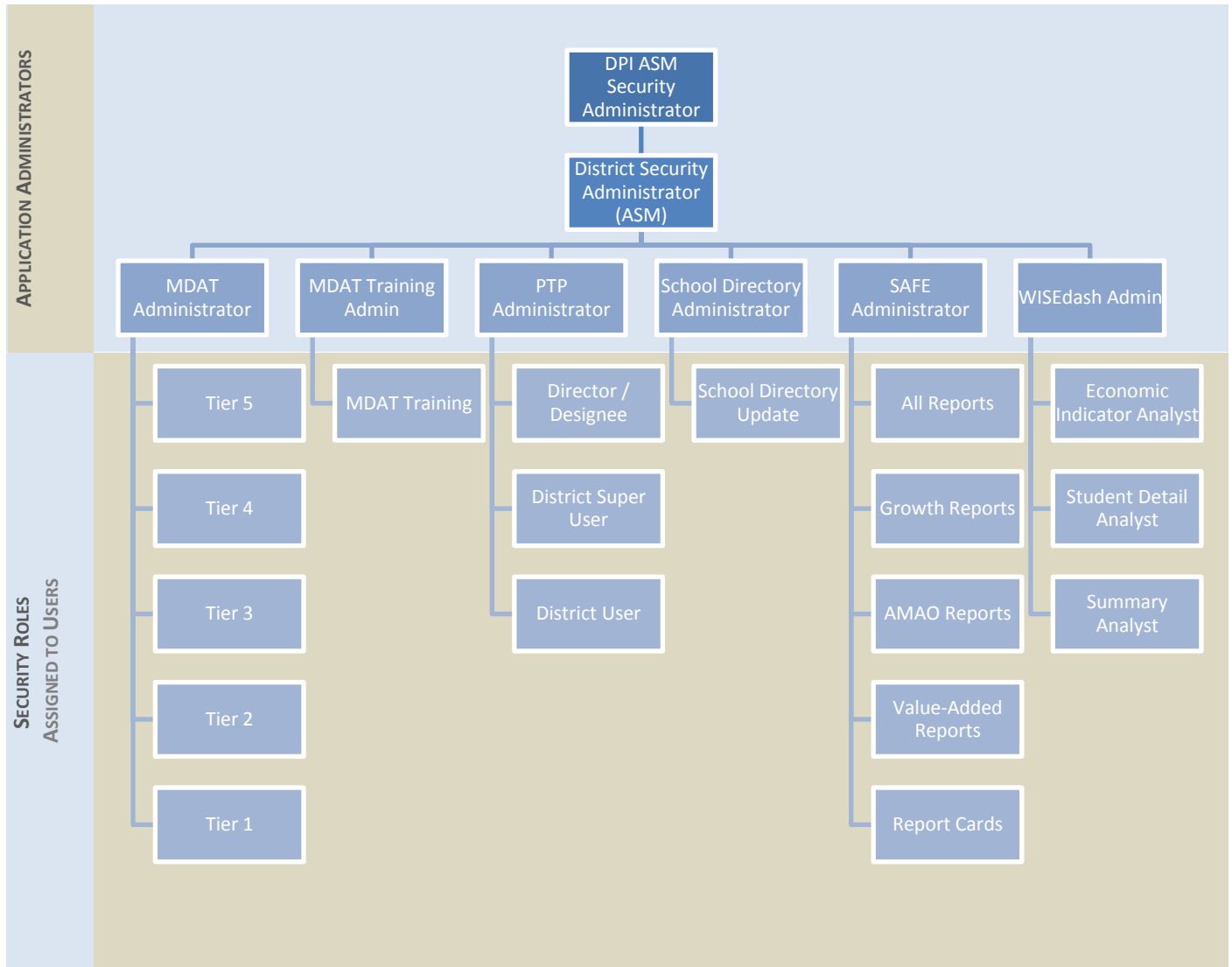
Secure Access File Exchange (SAFE)

An application that allows authorized users to access confidential data files and reports. Currently this application enables authorized access to the following topics: AMAO Report (District Profile), Student Growth Percentile (SGP) Reports and Value-Added Reports.

WISEdash

This application is a dashboard and reporting tool that allows users to access a wide variety of education data. Data included in the current version of WISEdash include enrollment and attendance, WSAS, ACT, AP and Student Growth Percentiles.   In this tool authorized users have the ability to search students by student name.

2. APPLICATIONS AND SECURITY ROLES

APPLICATION ADMINISTRATORS

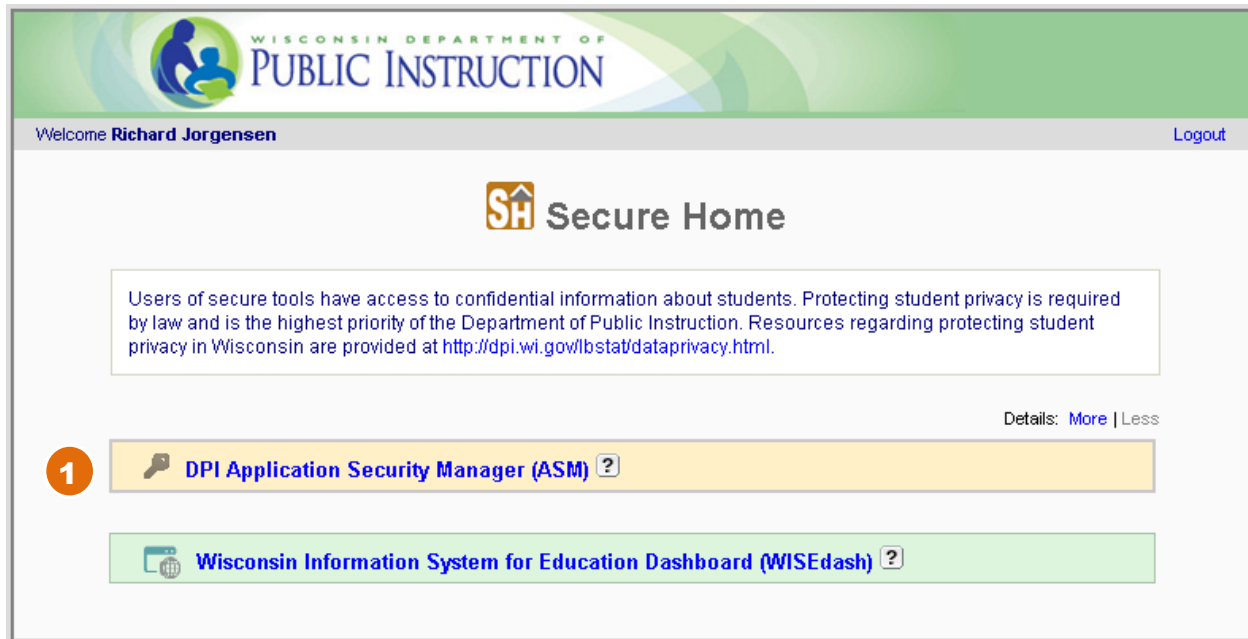DPI ASM Security Administrator

District Security Administrator (ASM)

| MDAT Administrator | MDAT Training Admin | PTP Administrator | School Directory Administrator | SAFE Administrator | WISEdash Admin |

SECURITY ROLES ASSIGNED TO USERS

MDAT Administrator	MDAT Training Admin	PTP Administrator	School Directory Administrator	SAFE Administrator	WISEdash Admin
Tier 5	MDAT Training	Director / Designee	School Directory Update	All Reports	Economic Indicator Analyst
Tier 4		District Super User		Growth Reports	Student Detail Analyst
Tier 3		District User		AMAO Reports	Summary Analyst
Tier 2				Value-Added Reports	
Tier 1				Report Cards	

3. APPLICATION AND SECURITY ROLES DEFINED

Roles	Roles Names in ASM	Application	Responsibility
DPI Security Administrator	ASM Role Admin	ASM	DPI provides access to the District Security Administrator.
District Security Administrator	ASM Role Admin	ASM	Delegate access to additional ASM users. An Application Administrator will need to be assigned for each application. For example, the District Security Administrator delegates the role of the Application Administrator for MDAT and SAFE.
PTP Application Administrator	IEP: PTP Role Admin	ASM	Manages access to the IEP: Postsecondary Transition Plan.
	District User	IEP: PTP	Enters student data and locks completed records.
	District Super User	IEP: PTP	Enters student data, locks completed records, unlocks completed records, submits records for DPI review.
	Director of Special Education/Designee	IEP: PTP	Enters student data, locks completed records, unlocks completed records, deletes unlocked records, submits records for DPI review, transfer student records between schools, match WSNs to students.
MDAT Application Administrator	MDAT Role Admin	ASM	Manages access to MDAT. Assigns Tiers 1, 2, 3, 4, or 5.
	MDAT Tier 1	MDAT	Student level, all variables, download option.
	MDAT Tier 2	MDAT	Student level, all variables.
	MDAT Tier 3	MDAT	Student level, no economic indicators.
	MDAT Tier 4	MDAT	Summary reports, all variables.
	MDAT Tier 5	MDAT	Summary reports, no economic indicators.
MDAT Training Application Administrator	MDAT Training Role Admin	ASM	Manages access to MDAT Training - all users get Tier 1 access.
SAFE Application Administrator	SAFE Role Admin	ASM	Manages access to SAFE. Assigns roles to view AMAO reports, growth reports, or all reports.
	ALL Reports	SAFE	View reports and files associated with all topics available in SAFE.
	Value-Added Reports	SAFE	View value added growth reports, access associated files.
	Accountability Report Cards	SAFE	View accountability report cards, access associated files.
	Student Growth Percentile Reports	SAFE	View student growth percentile reports, access associated files.
	AMAO Reports	SAFE	View AMAO district profile reports, access associated files
School Directory	School Directory DPI Admin	ASM	Manages access to the school directory

Application Administrator			application.
	School Directory Update	School Directory	View and update all district and school data for a district.
WISEdash Application Administrator	WISEdash Role Admin	ASM	Manages access to WISEdash. Assigns Summary Analyst, Student Detail Analyst, and Economic Indicator Analyst.
	Economic Indicator Analyst	WISEdash	View all summary dashboards, drill to the student list/student profile, utilize student search to access student profile, view the Economic Disadv Status filter, view the Econ Disadv Code and Econ Disadv Description on the Student Profile.
	Student Detail Analyst	WISEdash	View all summary dashboards, drill to the student list/student profile, utilize student search to access student profile. **Not** able to view the Economic Disadv Status filter or view Econ Disadv Code and Econ Disadv Description on the Student Profile.
	Summary Analyst	WISEdash	View all summary dashboards. **Not** able to drill to the student list/student profile or utilize student search to access student profile. **Not** able to view the Economic Disadv Status filter.

4. APPLICATION SECURITY MANAGER

4.1 LOGGING IN AND ASSIGNING ACCESS TO NEW USERS IN ASM

Login to ASM homepage using your WAMS ID and password: https://apps2.dpi.wi.gov/secure/

1 This is a list of secure applications you have access to. If this is your first time logging in, you may only see the **DPI Application Security Manager** in your list.

If you are the District Security Administrator, the DPI Application Security Manager application is where you will assign district Application Administrators for each application.

If you are a district Application Administrator, the DPI Application Security Manager is where you will provide yourself and other users with access to Secure Home applications: MDAT, MDAT Training, PTP, SAFE, School Directory and/or WISEdash.

After entering the **DPI Application Security Manager.** click on **2** **Add|Edit** above and to the right. The **Add|Edit Delegations** window appears. From the **3** **Application** drop down list, select the application you want to give the user access to.

Notes:

1. If you are a District Security Administrator, you will select "DPI Application Security Manager (ASM)" to assign an Application Administrator for an application.
2. If you are an Application Administrator and you **do not** see the application you want to grant access to in the drop down list, you are not the Application Administrator for that application.

Enter in the user's contact information and click **(4)** **Search.** Your results/records found will be listed in the box below your search. If more than one result is returned from your search, carefully review the list and **(5)** click on the radio button next to the user you want to give access to. Finally, click **(6)** **Select** to select the user to process.

.

Next, select the **(7)** **District** from the drop down box. The School, Available Roles and Current Roles window displays. Click on the checkbox next to the **(8)** **School(s)** you want the authority applied to. The **(9)** **Available Roles** and **(10)** **Current Roles** for the Application and User selected are displayed. If you need further information about the **Available Roles**, click on **View Role Descriptions** to see corresponding definitions.
Note:
1. To assign a role, click on the role in the **Available Roles** box and click the "**Add>>**" button.
2. To remove a role, click on the role in the **Current Roles** box and click the **"<<Remove"** button.

Make your final selections and click **(11)** **View Changes**. *This step does not yet confirm your selections.*

Following delegations were made

12

Wams ID	Name	Email	District	School	Application	Role	Delegation
dpiasmda07	Seven TestDisAdminSeven	dpiasmda07@dpi.wi.gov	Ashland	All Schools	DPIASM	ASM Role Admin	Granted

13 ☑ Notify **Seven TestDisAdminSeven** via email.

From: Richard.Jorgensen@dpi.wi.gov

Bcc: dpiasmda07@dpi.wi.gov

cc:

NOTE:multiple email addresses must be separated with commas.

Subject: Access to DPIASM Granted

This email is to notify you that you have been assigned access to DPI's Application Security Manager (ASM). As a user of ASM, you are responsible for managing either who else in your district may use ASM to manage access to secure applications (such as MDAT and SAFE), or who may use the specific secure applications.

ASM Role Admin - Ashland

There are two roles in Application Security Manager: ASM Administrator and Application Administrator.

ASM Administrators can log in to ASM to

- Delegate (or remove) people to/from the role of Application Administrator for for noth MDAT and SAFE. (Note:Each application-MDAT and SAFE-require seperate roles.)
- Delegate (or remove) people to/from the role of ASM Administrator for your district.
- In order to ensure detailed data security, roles require explicit assignment on an application basis. NOTE: ASM Administrators may also serve the role of Application Administrator for one or more applications. In such circumstances, the ASM Administrator should assign him/herself the appropriate additional roles.
- District Application Administrators can
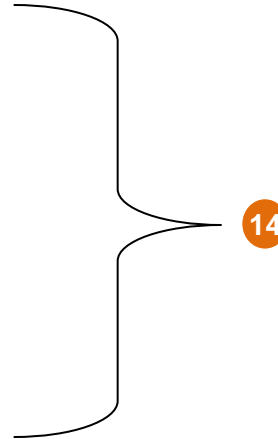
14

15 [Confirm Changes] [Change Delegations] [Cancel Changes]

View the knowledge base, or submit questions, comments, and suggestions to the Help Desk.

After selecting **View Changes,** a new window is displayed showing the **12** role selections, an **13** option to notify or not to notify the selected user about their new access, an **14** ASM generated email to the user, and an action to **15** **Confirm Changes**, **Change Delegations** or **Cancel Changes** for this request.

Note:

1. You may add additional email recipients by typing their email address in the email address fields.
2. **Confirm Changes** will send the email and complete the process. If you have chosen not to notify users by email, then this will just confirm changes.
3. **Change Delegations** will return you to the previous screen without changing the user's access.
4. **Cancel Changes** will cancel your action – nothing will be saved.

4.2 EDIT EXISTING USER ACCESS

Find the line of the Application, User, and District to change and click **1** **Edit.**

The **Available Roles** and **Current Roles** for the Application and User selected are displayed. You may **Add>>** or **<<Remove** assignments for the user and click **2** **View Changes**. *This step does not yet confirm your selections*.

After selecting **View Changes,** a new window is displayed showing the ③ role selections, an ④ option to notify or not to notify the selected user about their new access, an ⑤ ASM generated email to the user, and an action to ⑥ **Confirm Changes**, **Change Delegations** or **Cancel Changes** for this request.

Note:
1. You may add additional email recipients by typing their email address in the email address fields.
2. **Confirm Changes** will send the email and complete the process. If you have chosen not to notify users by email, then this will just confirm changes.
3. **Change Delegations** will return you to the previous screen without changing the user's access.
4. **Cancel Changes** will cancel your action – nothing will be saved.

4.3 REVOKING ACCESS FROM A CURRENT USER

Find the user(s) you want to remove access to and check the box under the **1** **Revoke** column to select the user. When you have completed selecting each user you want removed, click on the **2** **Revoke Selected** link.

Note:

1. You may revoke access from more than one user at a time.

Following delegations were made

AD ID	Name	Email	District	School	Application	Role	Delegation
jorgen4119	Richard Jorgensen	Richard.Jorgensen@dpi.wi.gov	All Districts	All Schools	DPIASM	ASM Role Admin	Revoked

☑ Notify via email.

From: Richard.Jorgensen@dpi.wi.gov

Bcc: This system sends emails to the address associated with a WAMS account. Please note that if one of the individuals listed below does not have an email address associated with his/her WAMS account, or if the email address given is not correct, he/she will not receive an email notification.

          Richard.Jorgensen@dpi.wi.gov

cc:

          NOTE:multiple email addresses must be separated with commas.

Subject: Access to Secure Tool(s) Revoked

This email is to notify you of a change to your secure access:
Your access to **<<Tool>>** has been revoked for **<<School/District>>**.

If you have any questions, please do not hesitate to contact the LDS team anytime. We may be reached through the LDS help desk tool: Footprints.

Sincerely,
The LDS Team

[Confirm Changes]   [Change Revoke Delegations]   [Cancel Changes]

View the knowledge base, or submit questions, comments, and suggestions to the Help Desk.

After selecting **Revoke Selected,** a new window is displayed showing the **3** role selections, an **4** option to notify or not to notify the selected user about their new access, an **5** ASM generated email to the user, and an action to **6** **Confirm Changes**, **Change Revoke Delegations** or **Cancel Changes** for this request.

Note:
1. You may add additional email recipients by typing their email address in the email address fields.
2. **Confirm Changes** will send the email and complete the process. If you have chosen not to notify users by email, then this will just confirm changes.
3. **Change Revoke Delegations** will return you to the previous screen without changing the user's access.
4. **Cancel Changes** will cancel your action – nothing will be saved.

4.4 LOGGING OUT

When you are finished always ① **Log Out** and close ALL browser windows.

Note: If you are assigning yourself access to a new application and/or role, you will need to log out and log back in to use your new access.